UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/621,060	07/21/2000	Dennis K. Branstad	NAI1P078/99.042.02	4286

28875 7590 06/04/2004

SILICON VALLEY INTELLECTUAL PROPERTY GROUP
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
ZIA, MOSSADEQ	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 06/04/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/621,060	BRANSTAD ET AL.	
	Examiner	Art Unit	
	Mossadeq Zia	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 July 2000*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13 and 24-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13 and 24-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-13 and 24-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Samar et al., "Unified Login with Pluggable Authentication Modules (PAM)" by Samar et al. in view of "Design and Implementation of Modular Key Management Protocol and IP Secure Tunnel on AIX" by Cheng et al. in further view of Patent No. 6,185,682 Tang.

3. Regarding claims 1, 11, Samar et al discloses a system for authenticating message data to be exchanged between a sender and a receiver, comprising:

a controller (API, Samar, page 1, para. 5, line 3) that dynamically selects one of a plurality of authentication mechanisms (authentication services, Samar, page 1, para. 5, line 4) to be used in providing authentication for an exchange of message data (response, Samar, page 3, 2nd to last para., last sentence);

but fail to show:

a security association and key management module that establishes security associations for said plurality of authentication mechanisms; and

an authentication module that includes support for said plurality of authentication mechanisms, wherein said authentication module generates an authentication tag using an

authentication mechanism selected by said control, said authentication tag being appended to said message data;

wherein a portion of a message associated with the message data is processed using a first function that is utilized at least in part to produce the authentication tag;

wherein said portion of said message processed is selected by using a pseudorandom probabilistic function.

However, Cheng et al. teaches a key management system, which teaches that security association between two communicating systems represents the information shared by systems in order to control a secure communication between them (security associations). This information includes secret keys, key life-times, nonces, crypto algorithms, parameters, etc., (Cheng, page 1, introduction, col. 1, last 3 sentences, col. 2, 1st sentence). Furthermore, a Message Authentication Code (authentication tag) [or integrity check function] which is applied to a piece of information (message data) for authentication (Cheng, page 3, section 2.1.1, col. 2, definition MAC_k, figure 4). Cheng also teaches if payload's (message data) integrity is to be protected, then a message authentication code (authentication tag) is computed on the concatenation of the IPST header (portion of a message associated with the message data) and the payload and is appended to the payload (Cheng, page 4, col. 2, 1st para.).

Tang teaches the construction means 120 derives the authentication control element from a small part of the entire set of authentication items. This may be done in various ways, like randomly (selected by using a pseudorandom probabilistic function) selecting some items or some bits of some items and using the selected parts directly or after a mixing operation as the authentication control element (Tang, col. 6, line 32-35).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Samar et al as per teaching of Cheng et al. and Tang such that the key management system will provide secure communication over the currently insecure Internet (Cheng, page 1, introduction, col. 1, para. 2, lines 2-3) and provide an authentication system which is simple to develop (Tang, col. 2, line 11-12).

4. Regarding claim 24, Samar, Cheng, and Tang shows claim 1 above, and further show message includes a number of message part, said message parts are 64-bit words [DES-CBC, page 5, col. 2, 1st para. It is well known in the art that DES-CBC processes 64 bit message blocks at a time).

5. Regarding claim 27, Samar, Cheng, and Tang shows claim 1 above, and further show first function is keyed hash function (Cheng, MAC_k, page 3, col. 2, middle of page, page 5, col. 1, 3rd para.).

6. Regarding claim 28, Samar, Cheng, and Tang shows claim 1 above, and further show first function is one of a MD4 hashing function, bucket hashing function, multi-linear modular hashing function, a cyclic redundancy code-based hashing function, and an alternative hash algorithm (Cheng, page 5, 1st para. "implemented as plug-in, replaceable modules and are not bound by DES-CBC and MD5").

7. Regarding claim 29, Samar, Cheng, and Tang shows claim 1 above, and further show portion of said message processed is selected by truncating message (plain text are processed in 64-bit under DES-CBC chunks, thus truncation of message must occur, therefore truncation of message is inherent in the system, see claim 24 for DES-CBC reference).

Allowable Subject Matter

8. Claim 25-26 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Arguments

9. Applicant's arguments with respect to claim 1-13 and 24-29 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

10. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mossadeq Zia whose telephone number is 703-305-8425. The examiner can normally be reached on Monday-Friday between 8:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 703-308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mossadeq Zia
Examiner
Art Unit 2134

mz
6/1/04

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100